

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA
CISCO

DIEGO FERNANDO LÓPEZ LEDEZMA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA SISTEMAS
BOGOTÁ
2022

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA
CISCO

DIEGO FERNANDO LOPEZ LEDEZMA

Diplomado de opción de grado presentado para optar el título de
INGENIERO SISTEMAS

DIRECTOR:
PAULITA FLOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA SISTEMAS
BOGOTÁ
2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTA, 22 de noviembre de 2022

TABLA DE CONTENIDO

| | |
|--|-----------|
| GLOSARIO | 8 |
| RESUMEN | 10 |
| ABSTRACT | 10 |
| INTRODUCCIÓN | 11 |
| 1. ESCENARIO 1 | 12 |
| 1.1 Esquema de direccionamiento..... | 13 |
| 1.2 Construcción en el simulador..... | 14 |
| 1.3 Configurar los aspectos básicos de los dispositivos de la Red propuesta ... | 15 |
| 1.3.1 Configuración R1..... | 16 |
| 1.3.2 Configuración S1..... | 20 |
| 1.4 Configurar los equipos host PC-A y PC-B..... | 25 |
| 1.4.1 Configuración host PC-A..... | 25 |
| 1.4.2 Configuración host PC-B..... | 27 |
| 1.5 Probar y verificar la conectividad de extremo a extremo..... | 29 |
| 2. Escenario 2 | 33 |
| 2.1 Construcción en el simulador..... | 35 |
| 2.2 Inicializar y volver a cargar el router y el switch..... | 35 |
| 2.3 Configure la plantilla SDM..... | 36 |
| 2.4 Configure R1..... | 37 |
| 2.5 Configure S1 y S2..... | 40 |
| 2.6 Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) | 43 |
| 2.7 Configurar soporte de host | 47 |
| 2.7.1 Configure R1..... | 47 |
| 2.8 Configurar los servidores..... | 49 |
| 2.9 Probar y verificar la conectividad de extremo a extremo..... | 51 |
| BIBLIOGRAFÍA | 58 |
| ANEXOS | 59 |
| ANEXO A – Enlace de descarga de las simulaciones de los escenarios..... | 59 |

LISTA DE TABLAS

| | |
|---|----|
| Tabla 1. Subredes definidas | 13 |
| Tabla 2. Esquema de direccionamiento | 13 |
| Tabla 3. Configuración R1 | 15 |
| Tabla 4. Comandos aplicados R1 | 17 |
| Tabla 5. Tareas realizar a S1 | 20 |
| Tabla 6. Comandos aplicados S1 | 22 |
| Tabla 7. Configuración red PC-A | 25 |
| Tabla 8. Configuración red Pc-B..... | 27 |
| Tabla 9. Verificación conectividad..... | 29 |
| Tabla 10. VLANS | 33 |
| Tabla 11. Esquema de direccionamiento | 34 |
| Tabla 12. Comandos aplicados R1, S1, S2. | 35 |
| Tabla 13. Comandos aplicados R1, S1, S2. | 36 |
| Tabla 14. Configuración a realizar R1 escenario 2 | 37 |
| Tabla 15. Configuración realizada R1 escenario 2 | 38 |
| Tabla 16. Configuración básica S1 y S2 | 40 |
| Tabla 17. Configuración realizada S1 | 41 |
| Tabla 18. Configuración realizada S2 escenario 2..... | 42 |
| Tabla 19. Configuración S1 escenario 2 | 43 |
| Tabla 20. Configuración realizada S1 escenario 2..... | 43 |
| Tabla 21. Configuración S2 escenario 2 | 45 |
| Tabla 22. Configuración realizada S2 escenario 2..... | 45 |
| Tabla 23. Configuración R1 escenario 2..... | 47 |
| Tabla 24. Configuración realizada R1 escenario 2 | 47 |
| Tabla 24. Configuración red de PC-A | 49 |
| Tabla 25. Configuración red de PC-B | 50 |
| Tabla 26. Verificación de conectividad..... | 51 |

LISTA DE FIGURAS

| | |
|--|----|
| Figura 1. Escenario 1 | 12 |
| Figura 2. Simulación creada en packet tracer..... | 14 |
| Figura 3. PC1 conectado a R1 | 16 |
| Figura 4. Conexión terminal desde PC1 a R1 | 16 |
| Figura 5 resultado de la configuración | 17 |
| Figura 6. PC0 Conectado a S1 | 21 |
| Figura 7. Conexión a terminal desde PC0 a S1 | 21 |
| Figura 8. Resultado comandos aplicados a S1 | 22 |
| Figura 9. Accediendo configuración red PC-A No 1 | 25 |
| Figura 10. Accediendo configuración red PC-A No 2..... | 26 |
| Figura 11. Ipconfig /all en PC-A | 26 |
| Figura 12. Accediendo configuración red PC-B No 1..... | 27 |
| Figura 13. Accediendo configuración red PC-B No 2..... | 28 |
| Figura 14. Ipconfig /all PC-B1 | 28 |
| Figura 15. Resultado final | 29 |
| Figura 16. Ping PC-A a R1 G0/0/0..... | 29 |
| Figura 17. Ping PC-A a R1 G0/0/1..... | 30 |
| Figura 18. Ping PC-A S1 VLAN1 | 30 |
| Figura 19. Ping PC-A a PC-B..... | 30 |
| Figura 20. Ping PC-B a R1 G0/0/0..... | 31 |
| Figura 21. Ping PC-B a R1 G0/0/1..... | 31 |
| Figura 22. Ping PC-B a VLAN1 | 31 |
| Figura 23. Prueba de Ping PC-A y PC-B | 32 |
| Figura 24. Escenario 2..... | 33 |
| Figura 25. Escenario 2 simulado en packet tracer | 35 |
| Figura 26. S1 y S2 Config prefer..... | 36 |
| Figura 27 ipconfig PC-A Escenario 2 | 49 |
| Figura 28 ipconfig PC-B Escenario 2 | 50 |
| Figura 29 ping IPV4 PC-A R1 G0/0/1.2 Escenario 2..... | 51 |
| Figura 30 ping IPV6 PC-A R1 G0/0/1.2 Escenario 2..... | 51 |
| Figura 31 ping IPV4 PC-A R1 G0/0/1.3 Escenario 2..... | 51 |
| Figura 32 ping IPV6 PC-A R1 G0/0/1.3 Escenario 2..... | 51 |
| Figura 33 ping IPV4 PC-A R1 G0/0/1.4 Escenario 2..... | 52 |
| Figura 34 ping IPV6 PC-A R1 G0/0/1.4 Escenario 2..... | 52 |
| Figura 35 ping IPV4 PC-A S1 VLAN4 Escenario 2 | 52 |
| Figura 36 ping IPV6 PC-A S1 VLAN4 Escenario 2 | 52 |
| Figura 37 ping IPV4 PC-A S2 VLAN4 Escenario 2 | 52 |
| Figura 38 ping IPV6 PC-A S2 VLAN4 Escenario 2 | 53 |
| Figura 39 ping IPV4 PC-A PC-B Escenario 2 | 53 |
| Figura 40 ping IPV6 PC-A PC-B Escenario 2 | 53 |
| Figura 41 ping IPV4 PC-A R1 BUCLE Escenario 2 | 53 |
| Figura 42 ping IPV6 PC-A R1 BUCLE Escenario 2 | 53 |

| | |
|---|----|
| Figura 43 ping IPV4 PC-B R1BUCLE Escenario 2 | 54 |
| Figura 44 ping IPV6 PC-B R1 BUCLE Escenario 2 | 54 |
| Figura 45 ping IPV4 PC-B R1 G0/0/1.2 Escenario 2..... | 54 |
| Figura 46 ping IPV6 PC-B R1 G0/0/1.2 Escenario 2..... | 54 |
| Figura 47 ping IPV4 PC-B R1 G0/0/1.3 Escenario 2..... | 54 |
| Figura 48 ping IPV6 PC-B R1 G0/0/1.3 Escenario 2..... | 55 |
| Figura 49 ping IPV4 PC-B R1 G0/0/1.4 Escenario 2..... | 55 |
| Figura 50 ping IPV6 PC-B R1 G0/0/1.4 Escenario 2..... | 55 |
| Figura 51 ping IPV4 PC-B S1 VLAN4 Escenario 2 | 55 |
| Figura 52 ping IPV6 PC-B S1 VLAN4 Escenario 2 | 55 |
| Figura 53 ping IPV4 PC-B S2 VLAN4 Escenario 2 | 56 |
| Figura 54 ping IPV6 PC-B S2 VLAN4 Escenario 2 | 56 |

GLOSARIO

802.11^a: Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 5 GHz.

802.11b: Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 11 Mbps y una frecuencia de funcionamiento de 2,4 GHz.

802.11g: Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 2,4 GHz y con compatibilidad con versiones anteriores con dispositivos 802.11b.

Adaptador: Dispositivo que añade funcionalidad de red a su equipo.

Ancho de banda: Capacidad de transmisión de un dispositivo o red determinado.

Banda ancha: Conexión a Internet de alta velocidad y siempre activa.

Bit (dígito binario): La unidad más pequeña de información de una máquina.

Byte: Una unidad de datos que suele ser de ocho bits.

Cifrado

Es la manipulación de datos para evitar que cualquiera de los usuarios a los que no están dirigidos los datos pueda realizar una interpretación precisa.

Método de autenticación mutua que utiliza una combinación de certificados digitales y otros sistemas, como contraseñas.

Conmutador: Dispositivo que es el punto central de conexión de equipos y otros dispositivos de una red, de forma que los datos puedan transmitirse a velocidad de transmisión completa.

Data Networking: Estado al que se llega después de haber implementado una red de dispositivos de cómputo comúnmente denominada Red LAN, se dice que al estar conectados todos estos dispositivos se conforma una red de datos.

DDNS (Sistema dinámico de nombres de dominio): Permite albergar un sitio Web, servidor FTP o servidor de correo electrónico con un nombre de dominio fijo (por ejemplo, www.xyz.com) y una dirección IP dinámica.

Descargar: Recibir un archivo transmitido a través de una red.

DHCP (Protocolo de configuración dinámica de host): Protocolo que permite a un dispositivo de una red, conocido como servidor DHCP, asignar direcciones IP temporales a otros dispositivos de red, normalmente equipos.

Dirección IP: Dirección que se utiliza para identificar un equipo o dispositivo en una red.

Dirección IP dinámica: Dirección IP temporal que asigna un servidor DHCP.

Dirección IP estática: Dirección fija asignada a un equipo o dispositivo conectado a una red.

Dispersión de secuencia: Técnica de frecuencia de radio de banda ancha que se utiliza para la transmisión más fiable y segura de datos.

Enrutador: Dispositivo de red que conecta redes múltiples, tales como una red local e Internet.

Enrutamiento estático: Reenvío de datos de una red a través de una ruta fija.

Ethernet: Protocolo de red estándar de IEEE que especifica la forma en que se colocan los datos y se recuperan de un medio de transmisión común.

RESUMEN

Durante el desarrollo del presente documento se encontrará la solución a las dos situaciones propuestas como parte de la prueba final de habilidades prácticas en el Diplomado de profundización cisco (diseño e implementación de soluciones integradas lan / wan).

Mostrando paso a paso la configuración e interconexión de los dispositivos que forman parte de la red, de acuerdo a lo requerido en cada uno de los escenarios propuestos y reflejando su correcta implementación por medio de las pruebas realizadas para verificar su funcionamiento.

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

During the development of this document, the solution to the two situations proposed will be found as part of the final test of practical skills in the Cisco Deepening Diploma (design and implementation of lan / wan integrated solutions).

Showing step by step the configuration and interconnection of the devices that are part of the network, according to what is required in each of the proposed scenarios and reflecting its correct implementation through the tests carried out to verify its operation.

Keywords: CISCO, CCNA, Switching, Routing, Networks, Electronic
Keywords: CISCO, CCNA, Routing, Swicthing, Networking, Electronics.

INTRODUCCIÓN

Las redes hoy en día son elementos indispensables a la hora de permitir la intercomunicación ya sea de empresas, personas, gobiernos, etc. De acuerdo a cada una de las necesidades encontramos redes LAN, MAN, WAN y tipos de medios guiados o no guiados al igual que la topología y protocolos necesarios para su implementación.

Teniendo en claro los conceptos básicos encontramos que las redes para su implementación requieren de diferentes componentes ya sean hardware, software, medios de transmisión, servidores y clientes. Para comprender mejor el funcionamiento debemos profundizar y comprender el modelo OSI el cual proporciona estándares y divide el viaje de la información a través de la red en capas claramente identificadas como física, enlace de datos, red, transporte, sesión, presentación y aplicación. De igual manera es importante conocer los protocolos TCP/IP Y ETHERNET, las aplicaciones que incluye, el proceso de encapsulamiento de los paquetes de datos y el flujo de los mismos a través de las diferentes capas.

La solución del primer escenario fue simulada en la herramienta packet tracer, implementando la configuración en los diferentes dispositivos Router, switch, equipos de cómputo y vlans. Permitiendo la conectividad IPV4 entre los dispositivos que componen la red.

La solución al segundo escenario se simulo por medio de la herramienta packet tracer y se implementó la configuración para los dispositivos router, switches, equipos de computos, vlans, trunking, etherchannel y dhcp, permitiendo la conectividad IPV4, IPV6 entre los diferentes dispositivos que componen la red.

1. ESCENARIO 1

Escenario: En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

Figura 1. Escenario 1



Prueba de habilidades CCNA ii-2022

1.1 Esquema de direccionamiento.

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento

Tabla 1 Subredes definidas

| Red | Re q. | Dir red | Mascara | / | 1era ip | Ult ip | Broadca st | Host s |
|----------|----------|----------------|---------------------|--------|----------------|----------------|----------------|-----------|
| LAN 1 | 60 | 172.8.3. 0 | 255.255.255. 192 | 2 6 | 172.8.3. 1 | 172.8.3. 62 | 172.8.3. 63 | 62 |
| LAN 2 | 20 | 172.8.3. 64 | 255.255.255. 224 | 2 7 | 172.8.3. 65 | 172.8.3. 94 | 172.8.3. 95 | 30 |

Prueba de habilidades CCNA ii-2022

Tabla 2. Esquema de direccionamiento

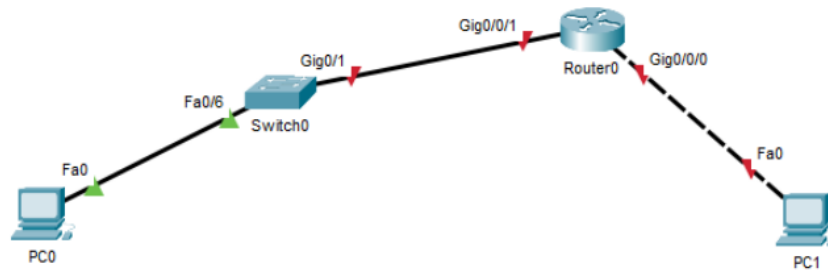
| Item | Requerimiento |
|-----------------------------------|---|
| Dirección de Red | 172.8.3.XY donde XY corresponde a los últimos dos dígitos de su cédula. (Tener en cuenta que esta red es publica) |
| Requerimiento de host Subred LAN1 | 60 |
| Requerimiento de host Subred LAN2 | 20 |
| R1 G0/0/1 | Última dirección de host de la subred LAN1 172.8.3.62 |
| R1 G0/0/0 | Última dirección de host de la subred LAN2 172.8.3.94 |
| S1 SVI | Segunda dirección de host de la subred LAN1 172.8.3.2 |
| PC-A | Décima dirección de host de la subred LAN1 172.8.3.10 |
| PC-B | Décima dirección de host de la subred LAN2 172.8.3.74 |

Prueba de habilidades CCNA ii-2022

1.2 Construcción en el simulador

Se crean los diferentes dispositivos en el simulador.

Figura 2. Simulación creada en packet tracer



Fuente Autoría propia

1.3 Configurar los aspectos básicos de los dispositivos de la Red propuesta

Las tareas de configuración para R1 incluyen las siguientes:

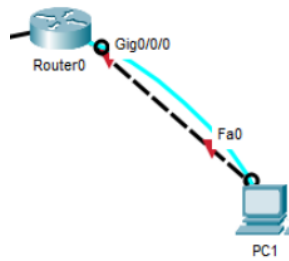
Tabla 3. Configuración R1

| Tarea | Especificación |
|---|--|
| Desactivar la búsqueda DNS | |
| Nombre del router | R1 |
| Nombre de dominio | ccna-sa.com |
| Contraseña cifrada para el modo EXEC privilegiado | ciscoenpass |
| Establecer la longitud mínima para las contraseñas | 10 caracteres |
| Crear un usuario administrativo en la base de datos local | Nombre de usuario: admin Contraseña: admin1pass |
| Configure el inicio de sesión en las líneas VTY para que use la base de datos local | |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | |
| Cifrar las contraseñas de texto no cifrado | |
| Configurar un banner MOTD | Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. |
| Configuración de interface G0/0/0 | Establecer la descripción Establecer la dirección IPv4 Activar la interfaz. |
| Configuración de interface G0/0/1 | Establecer la descripción Establecer la dirección IPv4 Activar la interfaz. |
| Generar una clave de cifrado RSA | Módulo de 1024 bits |

Fuente Autoría propia

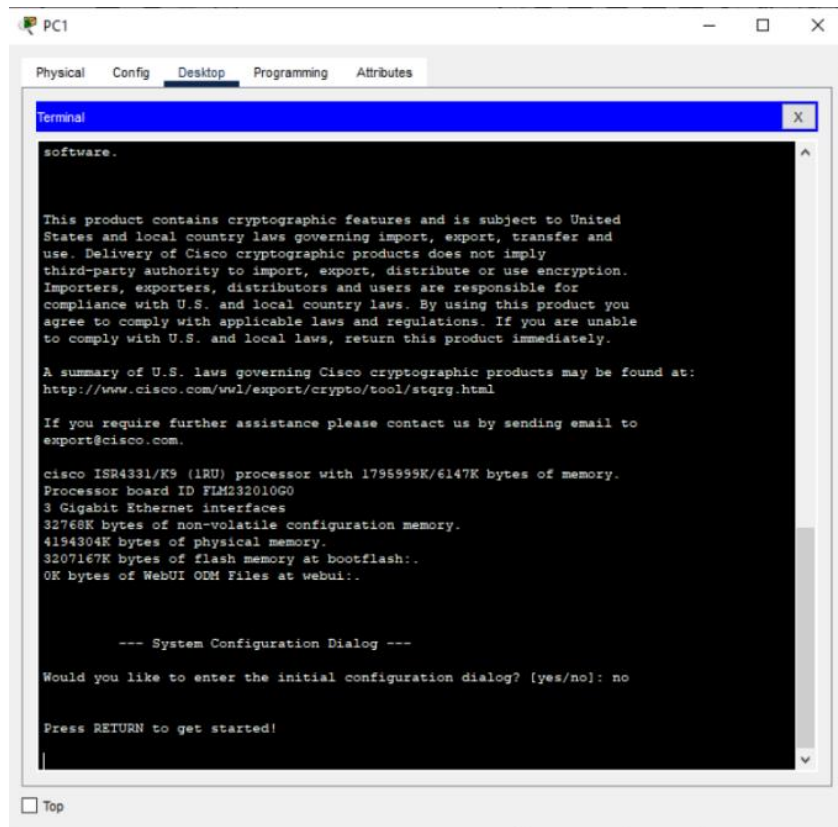
1.3.1 Configuración R1

Figura 3. PC1 conectado a R1



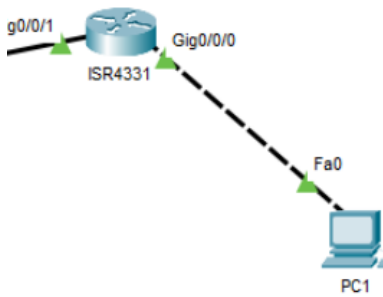
Fuente Autoría propia

Figura 4. Conexión terminal desde PC1 a R1



Fuente Autoría propia

Figura 5 resultado de la configuración



Diego Fernando Lopez.

Comandos aplicados

Tabla 4. Comandos aplicados R1

| Comando | Descripción |
|--|---|
| Router0 Router>enable | ingresamos modo privilegiado |
| Router0 Router#config terminal | cambiamos a modo configuración |
| Router0 Router(config)#hostname R1 | Asignamos el nombre al router |
| Router0 R1(config)#no ip domain-lookup | desactivamos la traducción de nombres a direcciones |
| Router0 R1(config)#ip domain-name ccna-sa.com | Especificamos el nombre de dominio |
| Router0 R1(config)#enable secret ciscoenpass | restringimos el acceso al modo EXEC privilegiado |
| Router0 R1(config)#line console 0 | Ingresamos a la opción línea comando |
| Router0 R1(config-line)#password ciscoenpass | restringimos el acceso al modo EXEC privilegiado |
| Router0 R1(config-line)#login | habilitamos la contraseña de seguridad |
| Router0 R1(config-line)#exit | Salimos de línea comando |
| Router0 R1(config)#security password min-length 10 | Establecemos el mínimo tamaño contraseña a 10 |

| | |
|---|---|
| Router0 R1(config)#username admin secret admin1pass | Creamos el usuario admin |
| Router0 R1(config)#line vty 0 15 | Ingresamos a configurar las sesiones telnet |
| Router0 R1(config-line)#login local | habilitamos la base de datos local |
| Router0 R1(config-line)#transport input ssh | Activación de SSH para el establecimiento de conexiones remotas |
| Router0 R1(config-line)#exit | Salida |
| Router0 R1(config)#service password- encryption | Habilitamos el cifrado de contraseña |
| Router0 R1(config)#banner motd % R1 Diego Fernando Lopez Ledezma Ing. sistemas Acceso denegado% | Creamos el mensaje en caso de error en el login al Router |
| Router0 R1(config)#do wr | Guardamos la configuración |
| Router0 R1(config)#int g0/0/1 | Seleccionamos la interfaz a configurar |
| Router0 R1(config-if)#ip address 172.8.3.62 255.255.255.192 | Asignamos la ip y mascara de red |
| Router0 R1(config-if)#no shutdown | Habilitamos la interfaz |
| Router0 R1(config-if)#int g0/0/0 | Seleccionamos la interfaz a configurar |
| Router0 R1(config-if)#ip address 172.8.3.94 255.255.255.224 | Asignamos la ip y mascara de red |
| Router0 R1(config-if)#no shutdown | Habilitamos la interfaz |
| Router0 R1(config-if)#exit | salida |
| Router0 R1(config)#crypto key generate rsa general-keys modulus 1024 | Creamos la clave de encriptación |
| Router0 R1(config)#do wr | Guardamos la configuración |
| Router0 R1(config)#int g0/0/0 | Seleccionamos la interfaz a configurar |
| Router0 R1(config-if)#description LAN2 | Agregamos la descripción a la interfaz |
| Router0 R1(config-if)#no shutdown | Habilitamos la interfaz |

| | |
|-----------------------------|----------------------------|
| Router0 R1(config-if)#do wr | Guardamos la configuración |
|-----------------------------|----------------------------|

Fuente Autoría propia

1.3.2 Configuración S1

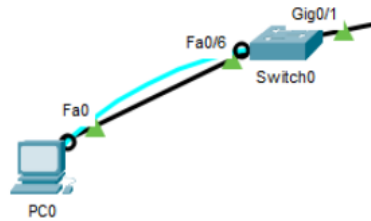
Las tareas de configuración para S1 incluyen las siguientes:

Tabla 5. Tareas realizar a S1

| Tarea | Especificación |
|---|--|
| Desactivar la búsqueda DNS | |
| Nombre del Router | S1 |
| Nombre de dominio | ccna-sa.com |
| Contraseña cifrada para el modo EXEC privilegiado | ciscoenpass |
| Apagar todos los puertos sin usar | F0/1-4, F0/7-24, G0/1-2 |
| Crear un usuario administrativo en la base de datos local | Nombre de usuario: admin Contraseña: admin1pass |
| Configure el inicio de sesión en las líneas VTY para que use la base de datos local | |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | |
| Cifrar las contraseñas de texto no cifrado | |
| Configurar un banner MOTD | Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. |
| Generar una clave de cifrado RSA | Módulo de 1024 bits |
| Configure la interfaz de administración (SVI) en VLAN1 | Establecer la descripción Establecer la dirección IPv4 |

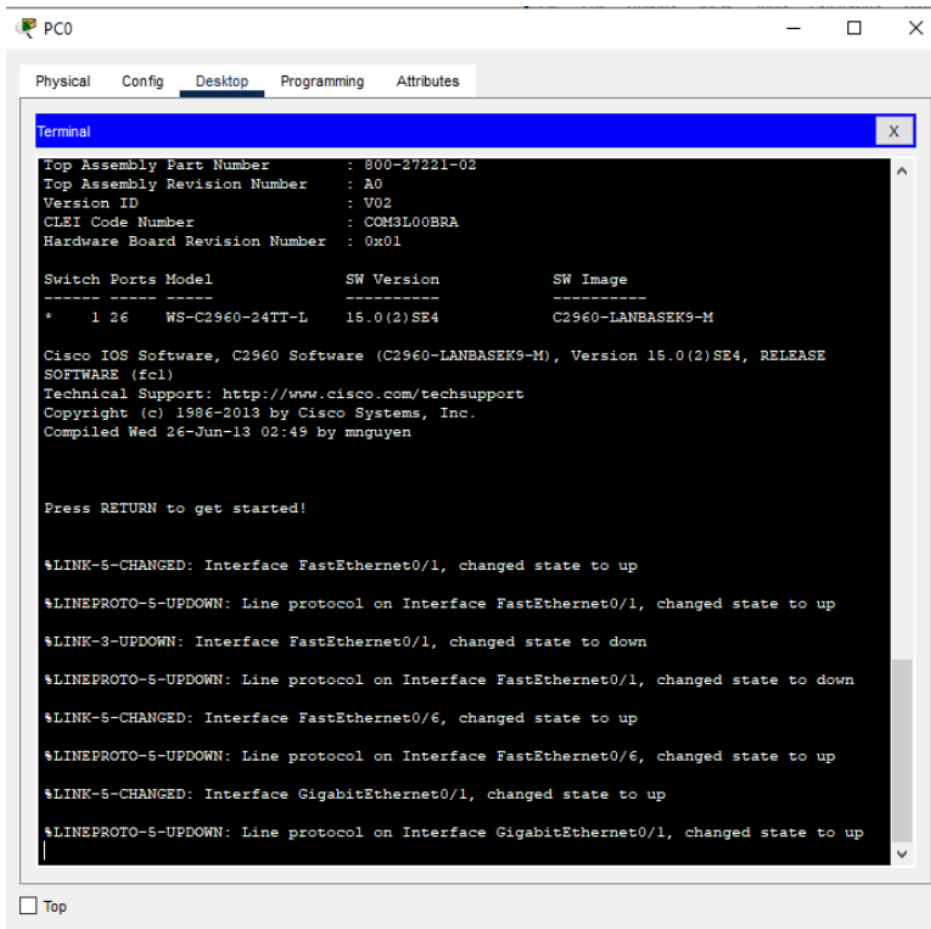
Fuente Autoría propia

Figura 6. PC0 Conectado a S1



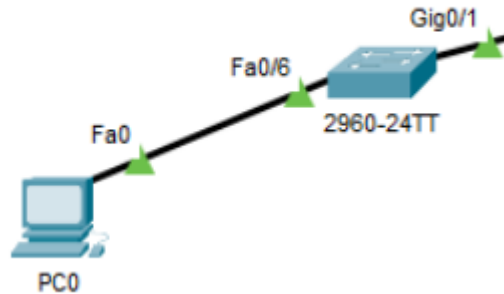
Fuente Autoría propia

Figura 7. Conexión a terminal desde PC0 a S1



Fuente Autoría propia

Figura 8. Resultado comandos aplicados a S1



Fuente Autoría propia

Comandos aplicados

Tabla 6. Comandos aplicados S1

| Comando | Explicación |
|---|---|
| Switch0 Switch>enable | ingresamos modo privilegiado |
| Switch0 Switch#config terminal | cambiamos a modo configuración |
| Switch0 Switch(config)#hostname S1 | Asignamos el nombre al router |
| Switch0 S1(config)#no ip domain-lookup | desactivamos la traducción de nombres a direcciones |
| Switch0 S1(config)#ip domain-name ccna-sa.com | Especificamos el nombre de dominio |
| Switch0 S1(config)#enable secret ciscoenpass | restringimos el acceso al modo EXEC privilegiado |
| Switch0 S1(config)#interface range fastEthernet 0/1-4 | seleccionamos las interfaces a modificar |

| | |
|--|---|
| Switch0 S1(config-if-range)#shutdown | deshabilitamos las interfaces seleccionada |
| Switch0 S1(config-if-range)#exit | salimos |
| Switch0 S1(config)#interface range fastEthernet 0/7-24 | seleccionamos las interfaces a modificar |
| Switch0 S1(config-if-range)#shutdown | Activamos las interfaces |
| Switch0 S1(config)#interface range g0/1-2 | seleccionamos las interfaces a modificar |
| Switch0 S1(config-if-range)#shutdown | Activamos las interfaces |
| Switch0 S1(config-if-range)#exit | salir |
| Switch0 S1(config)#line console 0 | Ingresamos a la opción line comando |
| Switch0 S1(config-line)#password ciscoenpass | restringimos el acceso al modo EXEC privilegiado |
| Switch0 S1(config-line)#login | Habilitamos contraseña |
| Switch0 S1(config-line)#exit | salir |
| Switch0 S1(config)#username admin secret admin1pass | Creamos el usuario admin |
| Switch0 S1(config)#line vty 0 15 | Ingresamos a configurar las sesiones telnet |
| Switch0 S1(config-line)#login local | habilitamos la base de datos local |
| Switch0 S1(config-line)#transport input ssh | Activación de SSH para el establecimiento de conexiones remotas |
| Switch0 S1(config-line)#service password-encryption | Salida |

| | |
|---|---|
| Switch0 S1(config)#banner motd % S1 Diego Fernando Lopez Ledezma Ing. Sistemas Acceso denegado% | Creamos el mensaje en caso de error en el login al Router |
| Switch0 S1(config)#crypto key generate rsa general-keys modulus 1024 | Creamos la clave de encriptación |
| Switch0 S1(config)#int vlan 1 | seleccionamos las interfaces a modificar |
| Switch0 S1(config-if)#description LAN1 | Agregamos la descripción a la interfaz |
| Switch0 S1(config-if)#ip address 172.8.3.2 255.255.255.192 | Asignamos la ip y mascara de red |
| Switch0 S1(config-if)#ip default-gateway 178.8.3.1 | Asignamos la puerta de enlace |
| Switch0 S1(config)#do wr | Guardamos la configuración |
| 2960-24TT S1(config)#int vlan 1 | seleccionamos las interfaces a modificar |
| 2960-24TT S1(config-if)#no shutdown | Activamos la interfaz |
| 2960-24TT S1(config-if)#do wr | Guardamos la configuración |
| 2960-24TT S1(config-if)#int g0/1 | seleccionamos las interfaces a modificar |
| 2960-24TT S1(config-if)#no shutdown | Activamos la interfaz |
| 2960-24TT S1(config-if)#do wr | Guardamos la configuración |

Fuente Autoría propia

1.4 Configurar los equipos host PC-A y PC-B

Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando ipconfig /all.

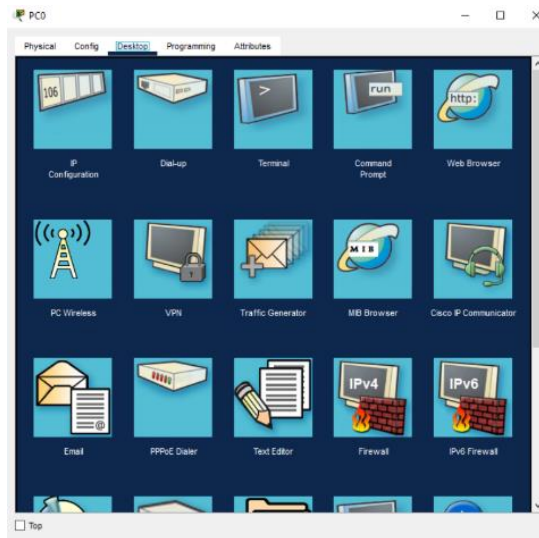
1.4.1 Configuración host PC-A

Tabla 7. Configuración red PC-A

| Configuración | |
|--------------------------------------|---|
| Descripción | FastEthernet0 Connection:(default port) |
| Dirección física | 0003.E4DA.98D8 |
| Dirección IPv4 | 172.8.3.10 |
| Máscara de subred | 255.255.255.192 |
| Puerta de enlace IPv4 predeterminada | 172.8.3.62 |

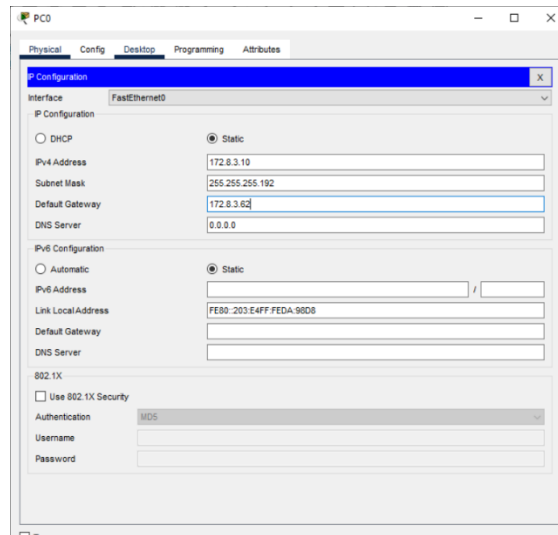
Fuente Autoría propia

Figura 9. Accediendo configuración red PC-A No 1



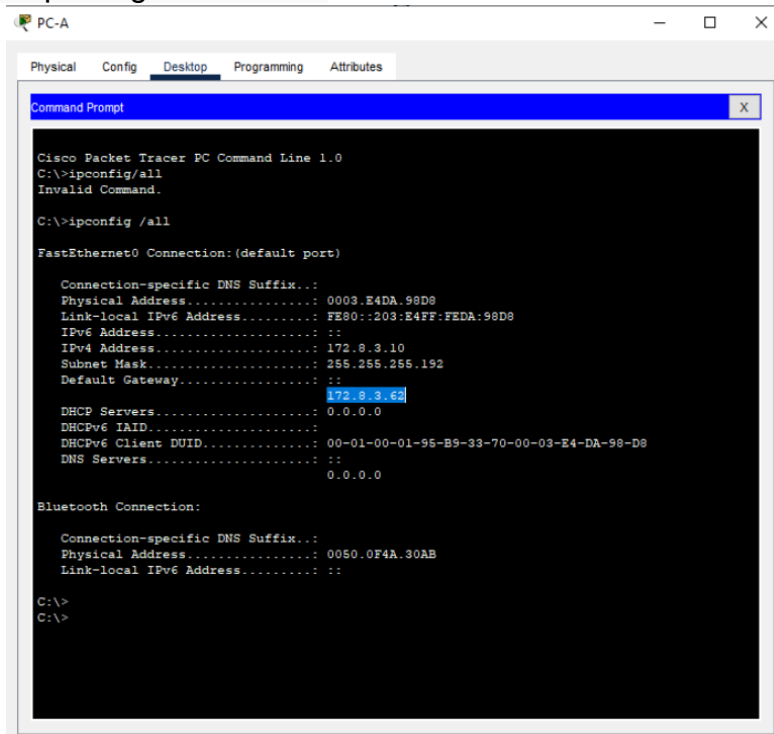
Fuente Autoría propia

Figura 10. Accediendo configuración red PC-A No 2



Fuente Autoría propia

Figura 11. Ipconfig /all en PC-A



Fuente Autoría propia

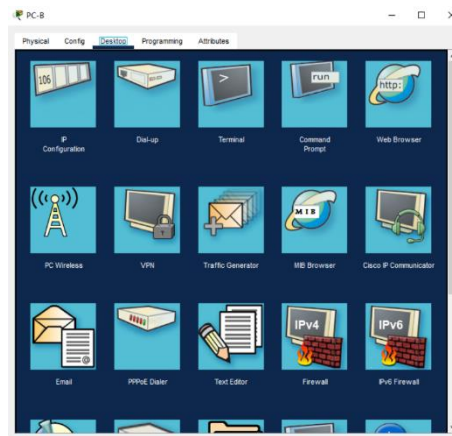
1.4.2 Configuración host PC-B

Tabla 8. Configuración red Pc-B

| Configuración de red de PC-B | |
|--------------------------------------|---|
| Descripción | FastEthernet0 Connection:(default port) |
| Dirección física | 00D0.97EA.D565 |
| Dirección IPv4 | 172.8.3.74 |
| Máscara de subred | 255.255.255.224 |
| Puerta de enlace IPv4 predeterminada | 172.8.3.94 |

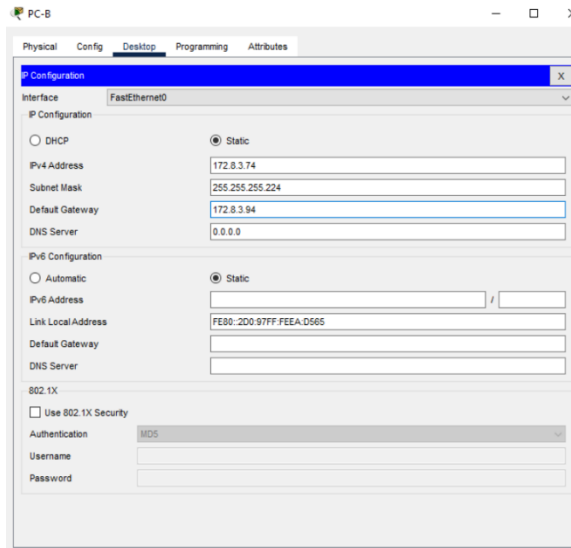
Fuente Autoría propia

Figura 12. Accediendo configuración red PC-B No 1



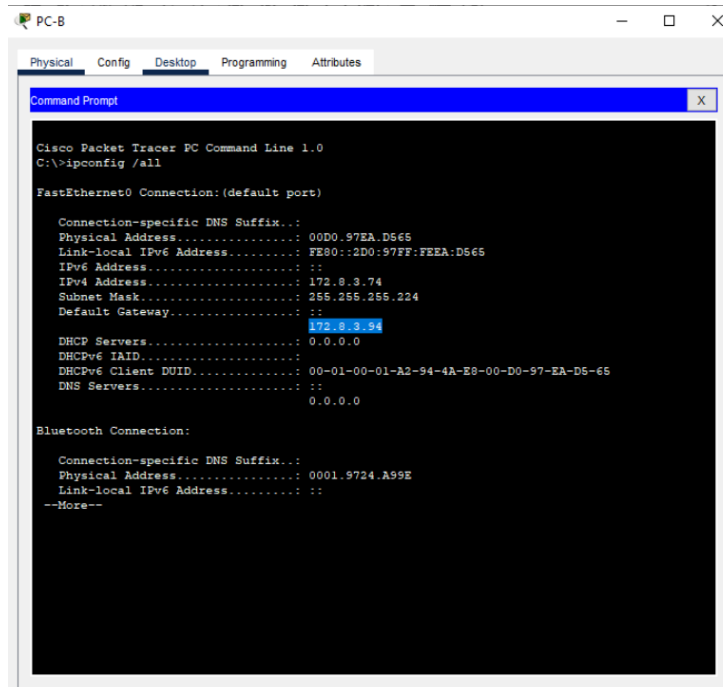
Fuente Autoría propia

Figura 13. Accediendo configuración red PC-B No 2



Fuente Autoría propia

Figura 14. Ipconfig /all PC-B1

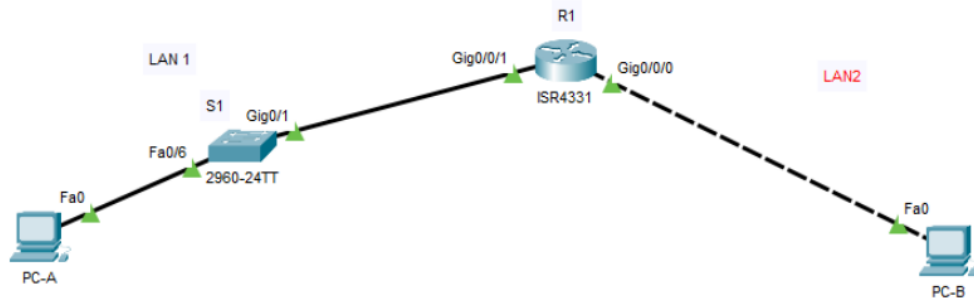


Fuente Autoría propia

1.5 Probar y verificar la conectividad de extremo a extremo.

Utilice el comando ping para probar la conectividad entre todos los dispositivos de red.

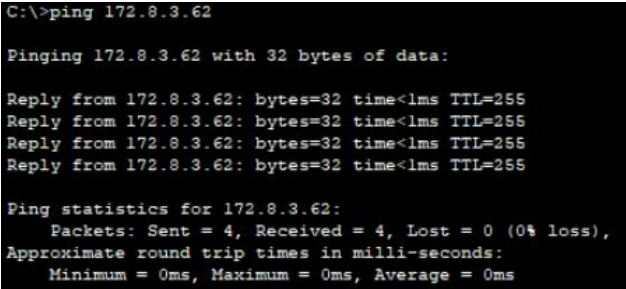
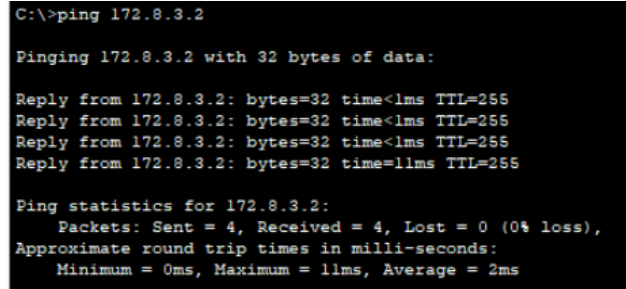
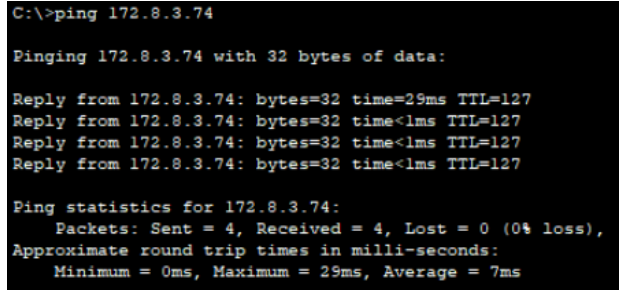
Figura 15. Resultado final

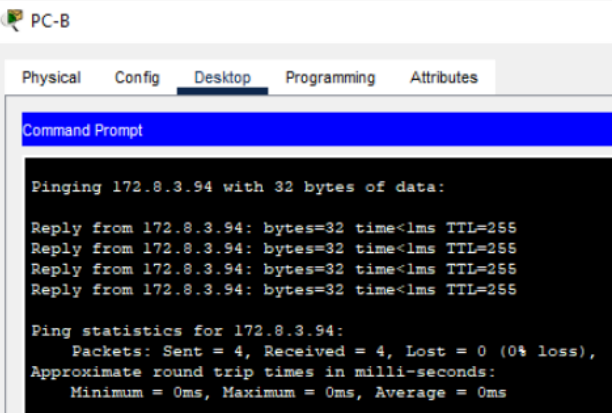
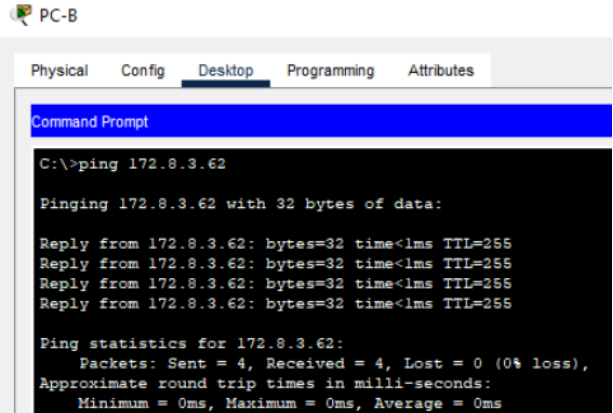
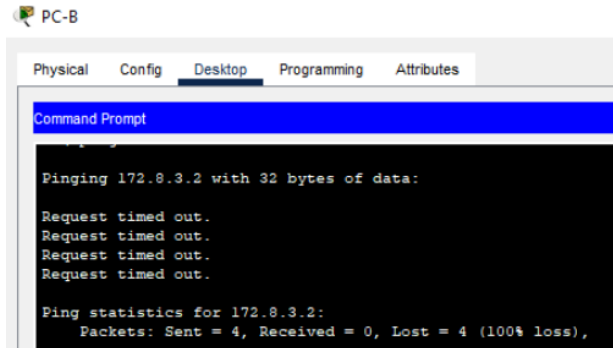


Fuente Autoría propia

Tabla 9. Verificación conectividad

| Desde | A | Dirección IP | Resultados de ping |
|-------|--------------|--------------|---|
| PC-A | R1 G0/0/0 | 172.8.3.94 | <p>Figura 16. Ping PC-A a R1 G0/0/0</p> <pre> C:\>ping 172.8.3.94 Pinging 172.8.3.94 with 32 bytes of data: Reply from 172.8.3.94: bytes=32 time<1ms TTL=255 Reply from 172.8.3.94: bytes=32 time<1ms TTL=255 Reply from 172.8.3.94: bytes=32 time<1ms TTL=255 Reply from 172.8.3.94: bytes=32 time<1ms TTL=255 Ping statistics for 172.8.3.94: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms </pre> <p>Fuente Autoría propia</p> |

| | | |
|--------------|------------|---|
| R1 G0/0/1 | 172.8.3.62 | <p>Figura 17. Ping PC-A a R1 G0/0/1</p>  <p>Fuente Autoría propia</p> |
| S1 VLAN 1 | 172.8.3.2 | <p>Figura 18. Ping PC-A S1 VLAN1</p>  <p>Fuente Autoría propia</p> |
| PC-B | 172.8.3.74 | <p>Figura 19. Ping PC-A a PC-B</p>  <p>Fuente Autoría propia</p> |

| | | | |
|------|--------------|------------|--|
| PC-B | R1 G0/0/0 | 172.8.3.94 | <p>Figura 20. Ping PC-B a R1 G0/0/0</p>  <p>Fuente Autoría propia</p> |
| | R1 G0/0/1 | 172.8.3.62 | <p>Figura 21. Ping PC-B a R1 G0/0/1</p>  <p>Fuente Autoría propia</p> |
| | S1 VLAN1 | 172.8.3.2 | <p>Figura 22. Ping PC-B a VLAN1</p>  <p>Fuente Autoría propia</p> |

Fuente Autoría propia

Figura 23. Prueba de Ping PC-A y PC-B

The screenshot shows a network simulation environment. The main window displays a topology with the following components and connections:

- PC-A** is connected to **S1** (Switch) via a **Fa0/24** interface.
- S1** is connected to **R1** (Router) via a **Gig0/1** interface.
- R1** is connected to **PC-B** via a **Gig0/0** interface.
- The network is divided into **LAN1** (containing PC-A and S1) and **LAN2** (containing R1 and PC-B).

The **Event List** window shows the following data:

| Vis. | Time(sec) | Last Device | AI Device |
|-------|-----------|-------------|-----------|
| 0.003 | 2960-24TT | PC-A | PC-A |
| 0.003 | SR4331 | PC-B | PC-B |
| 0.004 | PC-A | 2960-24TT | 2960-24TT |
| 0.004 | PC-B | SR4331 | SR4331 |
| 0.005 | 2960-24TT | SR4331 | SR4331 |
| 0.005 | SR4331 | 2960-24TT | 2960-24TT |
| 0.006 | SR4331 | PC-B | PC-B |
| 0.006 | 2960-24TT | PC-A | PC-A |
| 0.997 | - | 2960-24TT | 2960-24TT |
| 0.998 | 2960-24TT | SR4331 | SR4331 |
| 0.998 | 2960-24TT | PC-A | PC-A |
| 2.997 | - | 2960-24TT | 2960-24TT |
| 2.998 | 2960-24TT | SR4331 | SR4331 |
| 2.998 | 2960-24TT | PC-A | PC-A |
| 4.999 | - | 2960-24TT | 2960-24TT |

The **PDU List Window** shows the following data:

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delete |
|------|-------------|--------|-------------|------|--------|-----------|----------|-----|--------|----------|
| ● | Successful | PC-B | PC-A | ICMP | Orange | 0.000 | N | 0 | (edit) | (delete) |
| ● | Successful | PC-A | PC-B | ICMP | Black | 0.000 | N | 1 | (edit) | (delete) |

The **Simulation Panel** includes controls for **Reset Simulation**, **Constant Delay**, and **Play Controls** (Play, Stop, Pause, Previous, Next).

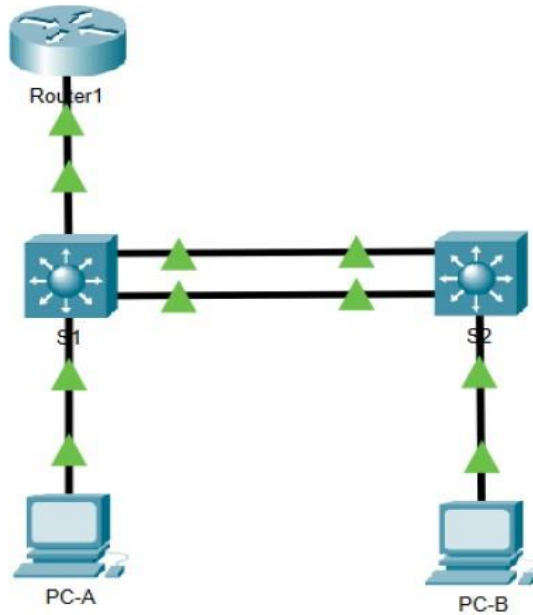
Fuente Autoría propia

Se realizaron pruebas de conexión mediante el comando ping entre el PC-A y interfaces de conexión del R1, S1 y PC-B permitiendo verificar la correcta conectividad entre los mismo.

De igual manera se realizaron pruebas para verificar conexión entre PC-B e interfaces de R1, S1 permitiendo verificar la correcta conectividad entre los mismo.

2. Escenario 2

Figura 24. Escenario 2



Prueba de habilidades CCNA ii-2022

En este escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configuraré el enrutamiento entre VLAN, DHCP, Etherchannel y port-security

Tabla 10. VLANS

| VLAN | Nombre de la VLAN |
|------|-------------------|
| 20 | Docentes |
| 30 | Estudiantes |
| 40 | Invitados |
| 50 | Usuarios |
| 56 | Native |

Prueba de habilidades CCNA ii-2022

Tabla 11. Esquema de direccionamiento

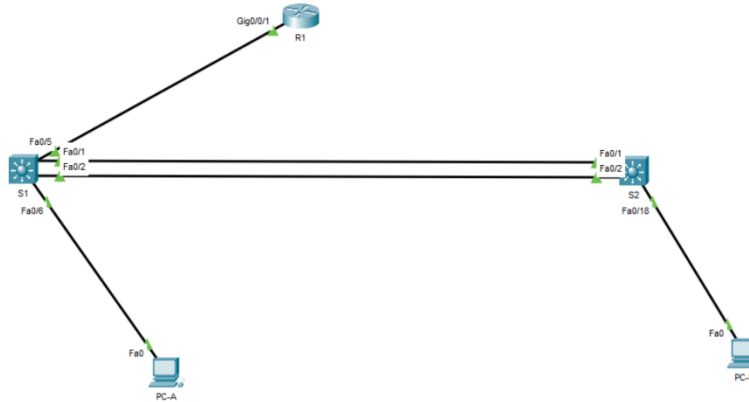
| Dispositivo / interfaz | Dirección IP / Prefijo | Puerta de enlace predeterminada |
|---|---------------------------|--|
| R1 G0/0/1.2 <i>R1 G0/0/1.2</i> | 10.8.8.1 /26 | No corresponde |
| | 2001:db8:acad:a: :1 /64 | No corresponde |
| R1 G0/0/1.3 | 10.8.8.65 /27 | No corresponde |
| <i>R1 G0/0/1.3</i> | 2001:db8:acad:b: :1 /64 | No corresponde |
| R1 G0/0/1.4 <i>R1 G0/0/1.4</i> | 10.8.8.97 /29 | No corresponde |
| | 2001:db8:acad:c: :1 /64 | No corresponde |
| R1 G0/0/1.6 | No corresponde | No corresponde |
| R1 Loopback0 <i>R1 Loopback0</i> | 209.165.201.1 /27 | No corresponde |
| | 2001:db8:acad:209: :1 /64 | No corresponde |
| S1 VLAN 4 | 10.8.8.98 /29 | 10.19.8.97 |
| <i>VLAN S1 4</i> | 2001:db8:acad:c: :98 /64 | No corresponde |
| <i>S1 VLAN 4</i> | fe80: :98 | No corresponde |
| S2 VLAN 4 <i>S2 VLAN 4</i> <i>S2 VLAN 4</i> | 10.8.8.99 /29 | 10.19.8.97 |
| | 2001:db8:acad:c: :99 /64 | No corresponde |
| | fe80: :99 | No corresponde |
| PC-A NIC | Dirección DHCP para IPv4 | DHCP para puerta de enlace predeterminada IPv4 |
| <i>PC-A NIC</i> | 2001:db8:acad:a: :50 /64 | fe80::1 |
| PC-B NIC <i>PC-B NIC</i> | DHCP para dirección IPv4 | DHCP para puerta de enlace predeterminada IPv4 |
| | 2001:db8:acad:b: :50 /64 | fe80::1 |

Prueba de habilidades CCNA ii-2022

Nota: No hay ninguna interfaz en el router que admita VLAN 50.

2.1 Construcción en el simulador

Figura 25. Escenario 2 simulado en packet tracer



Fuente Autoría propia

2.2 Inicializar y volver a cargar el router y el switch

Tabla 12. Comandos aplicados R1, S1, S2.

| Dispositivo | Comando | Explicación |
|-------------|-----------------------------|---|
| R1 | Router>delete vlan.data | Borrar la configuración de las VLANs del router |
| R1 | Router>erase startup-config | Borrar la configuración del Router |
| S1 | Switch> delete vlan.data | Borrar la configuración de las VLANs del switch 1 |
| S1 | Switch>erase startup-config | Borrar la configuración del switch 1 |
| S2 | Switch> delete vlan.data | Borrar la configuración de las VLANs del switch 2 |
| S2 | Switch>erase startup-config | Borrar la configuración del switch 2 |

Fuente Autoría propia

2.3 Configure la plantilla SDM.

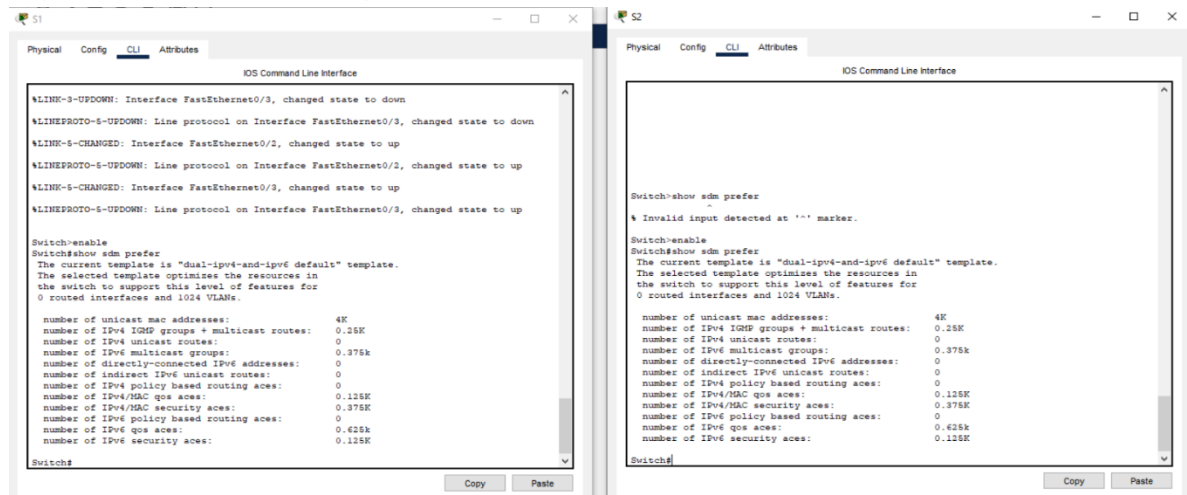
configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

Tabla 13. Comandos aplicados R1, S1, S2.

| Dispositivo | Comando | Explicación |
|-------------|---|--|
| R1 | Router>sdm prefer dual-ipv4-and-ipv6 default | Activa plantilla sdm para IPV6 y IPV4 del Router 1 |
| S1 | Switch> sdm prefer dual-ipv4-and-ipv6 default | Activa plantilla sdm para IPV6 y IPV4 del switch 1 |
| S2 | Switch> sdm prefer dual-ipv4-and-ipv6 default | Activa plantilla sdm para IPV6 y IPV4 del switch 2 |

Fuente Autoría propia

Figura 26. S1 y S2 Config prefer



Fuente Autoría propia

2.4 Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14. Configuración a realizar R1 escenario 2

| Tarea | Especificación |
|---|---|
| Desactivar la búsqueda DNS | |
| Nombre del router | R1 |
| Nombre de dominio | ccna-sa.com |
| Contraseña cifrada para el modo EXEC privilegiado | class |
| Contraseña de acceso a la consola | cisco |
| Establecer la longitud mínima para las contraseñas | 5 caracteres |
| Crear un usuario administrativo en la base de datos local | Nombre de usuario: admin Contraseña: admin1pass |
| Configure el inicio de sesión en las líneas VTY para que use la base de datos local | |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | |
| Cifrar las contraseñas de texto no cifrado | |
| Configurar un banner MOTD | Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. |
| Habilitar el routing IPv6 | |
| Configuración de interface G0/0/1 | Establecer la descripción Establecer la dirección IPv4 Establecer la dirección local de enlace IPv6 como fe80: :1 Establecer la dirección IPv6 Activar la interfaz. |
| Configure el Loopback0 interface | Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1 |
| Generar una clave de cifrado RSA | Módulo de 1024 bits |

Fuente Autoría propia

Tabla 15. Configuración realizada R1 escenario 2

| Tarea | Comandos |
|---|---|
| Desactivar la búsqueda DNS | Router(config)#no ip domain-lookup |
| Nombre del router | Router(config)#hostname R1 |
| Nombre de dominio | R1(config)#ip domain-name ccna-sa.com |
| Contraseña cifrada para el modo EXEC privilegiado | R1(config)#enable secret class |
| Contraseña de acceso a la consola | R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login |
| Establecer la longitud mínima para las contraseñas | R1(config)#security passwords min-length 5 |
| Crear un usuario administrativo en la base de datos local | R1(config)#username admin secret admin1pass |
| Configure el inicio de sesión en las líneas VTY para que use la base de datos local | R1(config)#line vty 0 15 R1(config-line)#login local R1(config-line)#exit |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#transport input ssh R1(config-line)#exit |
| Cifrar las contraseñas de texto no cifrado | R1(config)#service password-encryption |
| Configurar un banner MOTD | R1(config)#banner motd #R1, Diego Fernando Lopez, Ing sistemas. Acceso no autorizado # |
| Habilitar el routing IPv6 | R1(config)#IPv6 unicast-routing |
| Configuración de interface G0/0/1 | Subinterface 2: R1(config)#interface gigabitEthernet 0/0/1.2 R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#ip address 10.8.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#description Docentes R1(config-subif)#no shutdown Subinterface 3 R1(config)#interface gigabitEthernet 0/0/1.3 R1(config-subif)#encapsulation dot1Q 3 |

| | |
|----------------------------------|---|
| | <pre> R1(config-subif)#ip address 10.8.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#description Estudiantes R1(config-subif)#no shutdown Subinterface 4 R1(config)#interface gigabitEthernet 0/0/1.4 R1(config-subif)#encapsulation dot1Q 4 R1(config-subif)#ip address 10.8.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#description Invitados R1(config-subif)#no shutdown Subinterface 5 R1(config)#interface gigabitEthernet 0/0/1.5 R1(config-subif)#encapsulation dot1Q 5 R1(config-subif)#description Usuarios R1(config-subif)#no shutdown Subinterface 6 R1(config)#interface gigabitEthernet 0/0/1.6 R1(config-subif)#encapsulation dot1Q 6 R1(config-subif)#description Native R1(config-subif)#no shutdown </pre> |
| Configure el Loopback0 interface | <pre> R1(config)#interface loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#exit R1(config)#interface loopback 0 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 </pre> |
| Generar una clave de cifrado RSA | <pre> crypto key generate rsa </pre> |

Fuente Autoría propia

2.5 Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 16. Configuración básica S1 y S2

| Tarea | Especificación |
|---|---|
| Desactivar la búsqueda DNS | |
| Nombre del router | S1 o S2 según proceda |
| Nombre de dominio | ccna-sa.com |
| Contraseña cifrada para el modo EXEC privilegiado | class |
| Contraseña de acceso a la consola | cisco |
| Crear un usuario administrativo en la base de datos local | Nombre de usuario: admin Contraseña: admin1pass |
| Configure el inicio de sesión en las líneas VTY para que use la base de datos local | |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | |
| Cifrar las contraseñas de texto no cifrado | |
| Configurar un banner MOTD | Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. |
| Generar una clave de cifrado RSA | Módulo de 1024 bits |
| Configure la interfaz de administración (SVI) en VLAN1 | Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3 |
| Configuración del gateway predeterminado | Configure la puerta de enlace predeterminada como 10.XY.8.97 para IPv4 |

Fuente Autoría propia

Tabla 17. Configuración realizada S1

| Tarea | comandos |
|---|--|
| Desactivar la búsqueda DNS | Switch(config)#no ip domain-lookup |
| Nombre del router | Switch(config)#hostname S1 |
| Nombre de dominio | S1(config)#ip domain-name ccna-sa.com |
| Contraseña cifrada para el modo EXEC privilegiado | enable secret class |
| Contraseña de acceso a la consola | S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login |
| Crear un usuario administrativo en la base de datos local | S1(config)#username admin secret admin1pass |
| Configure el inicio de sesión en las líneas VTY para que use la base de datos local | S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#transport input ssh S1(config-line)#exit |
| Cifrar las contraseñas de texto no cifrado | S1(config)#service password-encryption |
| Configurar un banner MOTD | S1(config)#banner motd # S1, Diego Fernando Lopez, Ing. Sistemas, acceso no autorizado # |
| Generar una clave de cifrado RSA | S1(config)#crypto key generate rsa |
| Configure la interfaz de administración (SVI) | S1(config)#int vlan 40 S1(config-if)#ip address 10.8.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#no shutdown S1(config-if)#exit |
| Configuración del gateway predeterminado | S1(config)# ip default-gateway 10.8.8.97 |

Fuente Autoría propia

Tabla 18. Configuración realizada S2 escenario 2

| Tarea | Especificación |
|---|--|
| Desactivar la búsqueda DNS | Switch(config)#no ip domain-lookup |
| Nombre del router | Switch(config)#hostname S2 |
| Nombre de dominio | S2(config)#ip domain-name ccna-sa.com |
| Contraseña cifrada para el modo EXEC privilegiado | enable secret class |
| Contraseña de acceso a la consola | S2(config)#line console 0 S2(config-line)#password cisco S2(config-line)#login |
| Crear un usuario administrativo en la base de datos local | S2(config)#username admin secret admin1pass |
| Configure el inicio de sesión en las líneas VTY para que use la base de datos local | S2(config)#line vty 0 4 S2(config-line)#login local S2(config-line)#exit |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | S2(config)#line vty 0 4 S2(config-line)#login local S2(config-line)#transport input ssh S2(config-line)#exit |
| Cifrar las contraseñas de texto no cifrado | S2(config)#service password-encryption |
| Configurar un banner MOTD | S2(config)#banner motd # S2, Diego Fernando Lopez, Ing. Sistemas, acceso no autorizado # |
| Generar una clave de cifrado RSA | S2(config)#crypto key generate rsa |
| Configure la interfaz de administración (SVI) | S2(config)#int vlan 40 S2(config-if)#ip address 10.8.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#no shutdown S2(config-if)#exit |
| Configuración del gateway predeterminado | S2(config)# ip default-gateway 10.8.8.97 |

Fuente Autoría propia

2.6 Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Tabla 19. Configuración S1 escenario 2

| Tarea | Especificación |
|---|--|
| Crear VLAN | VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native |
| Crear troncos 802.1Q que utilicen la VLAN 6 nativa | Interfaces F0/1, F0/2 y F0/5 |
| Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 | Usar el protocolo LACP para la negociación |
| Configurar el puerto de acceso de host para VLAN 2 | Interface F0/6 |
| Configurar la seguridad del puerto en los puertos de acceso | Permitir 4 direcciones MAC |
| Proteja todas las interfaces no utilizadas | Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar |

Fuente Autoría propia

Tabla 20. Configuración realizada S1 escenario 2

| Tarea | comandos |
|------------|--|
| Crear VLAN | S1(config)#Vlan 20 S1(config-vlan)#name Docentes S1(config-vlan)#exit S1(config)#Vlan 30 S1(config-vlan)#name Estudiantes S1(config-vlan)#exit S1(config)#Vlan 40 S1(config-vlan)#name Invitados S1(config-vlan)#exit S1(config)#Vlan 50 S1(config-vlan)#name Usuarios S1(config-vlan)#exit S1(config)#Vlan 56 |

| | |
|--|--|
| | <pre>S1(config-vlan)#name Native S1(config-vlan)#exit</pre> |
| <p>Crear troncos 802.1Q que utilicen la VLAN 6 nativa</p> | <pre>S1(config)#interface range f0/1, f0/2, f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 56 S1(config-if-range)#switchport trunk allowed vlan 20,30,40,50,56 S1(config-if-range)# switchport trunk encapsulation dot1q S1(config-if)#exit</pre> |
| <p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p> | <pre>S1(config)#interface range fa0/1, fa0/2 S1(config-if-range)#channel-protocol lacp S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#exit</pre> |
| <p>Configurar el puerto de acceso de host para VLAN 2</p> | <pre>S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 20 S1(config-if)#no shutdown</pre> |
| <p>Configurar la seguridad del puerto en los puertos de acceso</p> | <pre>S1(config-if)#switchport mode access S1(config-if)#switchport port-security maximum 3 S1(config-if)#switchport port-security violation shutdown</pre> |
| <p>Proteja todas las interfaces no utilizadas</p> | <pre>S1(config-if)#interface range f0/3-4, f0/7-24, g0/1- 2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport acces vlan 50 S1(config-if-range)# description SW1- vlan50 S1(config-if-range)#shutdown</pre> |

Fuente Autoría propia

Tabla 21. Configuración S2 escenario 2

| Tarea | Especificación |
|---|--|
| Crear VLAN | VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native |
| Crear troncos 802.1Q que utilicen la VLAN 6 nativa | Interfaces F0/1, F0/2 |
| Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 | Usar el protocolo LACP para la negociación |
| Configurar el puerto de acceso de host para VLAN 2 | Interface F0/18 |
| Configurar la seguridad del puerto en los puertos de acceso | Permitir 4 direcciones MAC |
| Proteja todas las interfaces no utilizadas | Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar |

Fuente Autoría propia

Tabla 22. Configuración realizada S2 escenario 2

| Tarea | Comandos |
|--|---|
| Crear VLAN | S2(config)#Vlan 20 S2(config-vlan)#name Docentes S2(config-vlan)#exit S2(config)#Vlan 30 S2(config-vlan)#name Estudiantes S2(config-vlan)#exit S2(config)#Vlan 40 S2(config-vlan)#name Invitados S2(config-vlan)#exit S2(config)#Vlan 50 S2(config-vlan)#name Usuarios S2(config-vlan)#exit S2(config)#Vlan 56 S2(config-vlan)#name Native S2(config-vlan)#exit |
| Crear troncos 802.1Q que utilicen la VLAN 6 nativa | S2(config)#interface range f0/1, f0/2 S2(config-if)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 56 |

| | |
|--|--|
| | <pre>S2(config-if-range)#switchport trunk allowed vlan 20,30,40,50,56 S2(config-if-range)# switchport trunk encapsulation dot1q S2(config-if)#exit</pre> |
| <p>Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2</p> | <pre>S2(config)#interface range f0/1, f0/2 S2(config-if-range)#channel-protocol lacp S2(config-if-range)#channel-group 2 mode active S2(config-if-range)#exit</pre> |
| <p>Configurar el puerto de acceso de host para VLAN 3</p> | <pre>S2(config)#interface f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 30 S2(config-if)#no shutdown</pre> |
| <p>Configurar la seguridad del puerto en los puertos de acceso</p> | <pre>S2(config-if)#switchport mode Access S2(config-if)#switchport port-security maximum 3 S2(config-if)#switchport port-security violation shutdown</pre> |
| <p>Proteja todas las interfaces no utilizadas</p> | <pre>S2(config-if)#interface range f0/3-17, f0/19-24, g0/1- 2 S2 (config-if-range)#switchport acces vlan 50 S2(config-if-range)#switchport mode Access S2(config-if-range)#switchport nonegotiate S2(config-if-range)# description SW2-vlan50 S2(config-if-range)#shutdown</pre> |

Fuente Autoría propia

2.7 Configurar soporte de host

2.71 Configure R1

Tabla 23. Configuración R1 escenario 2

| Tarea | Especificación |
|-----------------------------------|---|
| Configure Default Routing | Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 |
| Configurar IPv4 DHCP para VLAN 20 | Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sa.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada |
| Configurar DHCP IPv4 para VLAN 30 | Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sb.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada |

Fuente Autoría propia

Tabla 24. Configuración realizada R1 escenario 2

| Tarea | Comandos |
|-----------------------------------|--|
| Configure Default Routing | R1(config)# ipv6 route ::/0 loopback 0 R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 |
| Configurar IPv4 DHCP para VLAN 20 | R1(config)#ip dhcp pool vlan 20 R1(dhcp-config)#network 10.8.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.8.8.1 R1(dhcp-config)#exit R1(dhcp-config)#domain-name unad-ccna-sa.net R1(dhcp-config)#dns-server 10.0.0.10 R1(dhcp-config)#exit |
| Configurar DHCP IPv4 para VLAN 30 | R1(config)#ip dhcp excluded-address 10.8.8.65 10.8.8.84 R1(config)#ip dhcp pool vlan 30 |

```
R1(dhcp-config)#network      10.8.8.64
255.255.255.224
R1(dhcp-config)#default-router 10.8.8.65
R1(dhcp-config)#domain-name  unad-
ccna-sa.net
R1(dhcp-config)#dns-server    10.0.0.10
R1(dhcp-config)#exit
R1# ip dhcp excluded-address 10.8.8.1
10.8.8.99
```

Fuente Autoría propia

2.8 Configurar los servidores

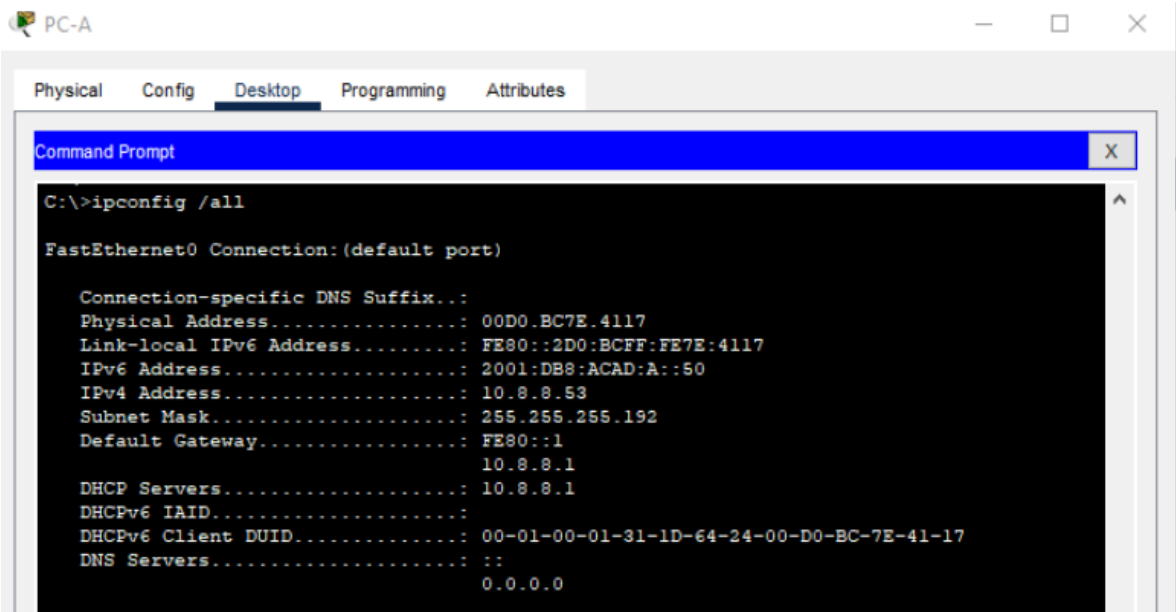
Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando ipconfig /all

Tabla 24. Configuración red de PC-A

| Configuración de red de PC-A | |
|------------------------------|-----------------|
| Descripción | |
| Dirección física | 00D0.BC7E.4117 |
| Dirección ip | 10.8.8.53 |
| Máscara de subred | 255.255.255.192 |
| Gateway predeterminado | 10.8.8.1 |
| Gateway predeterminado IPV6 | FE80::1 |

Fuente Autoría propia

Figura 27 ipconfig PC-A Escenario 2



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address...: 00D0.BC7E.4117
Link-local IPv6 Address...: FE80::2D0:BCFF:FE7E:4117
IPv6 Address...: 2001:DB8:ACAD:A::50
IPv4 Address...: 10.8.8.53
Subnet Mask...: 255.255.255.192
Default Gateway...: FE80::1
                  10.8.8.1
DHCP Servers...: 10.8.8.1
DHCPv6 IAID...:
DHCPv6 Client DUID...: 00-01-00-01-31-1D-64-24-00-D0-BC-7E-41-17
DNS Servers...: :
                  0.0.0.0
```

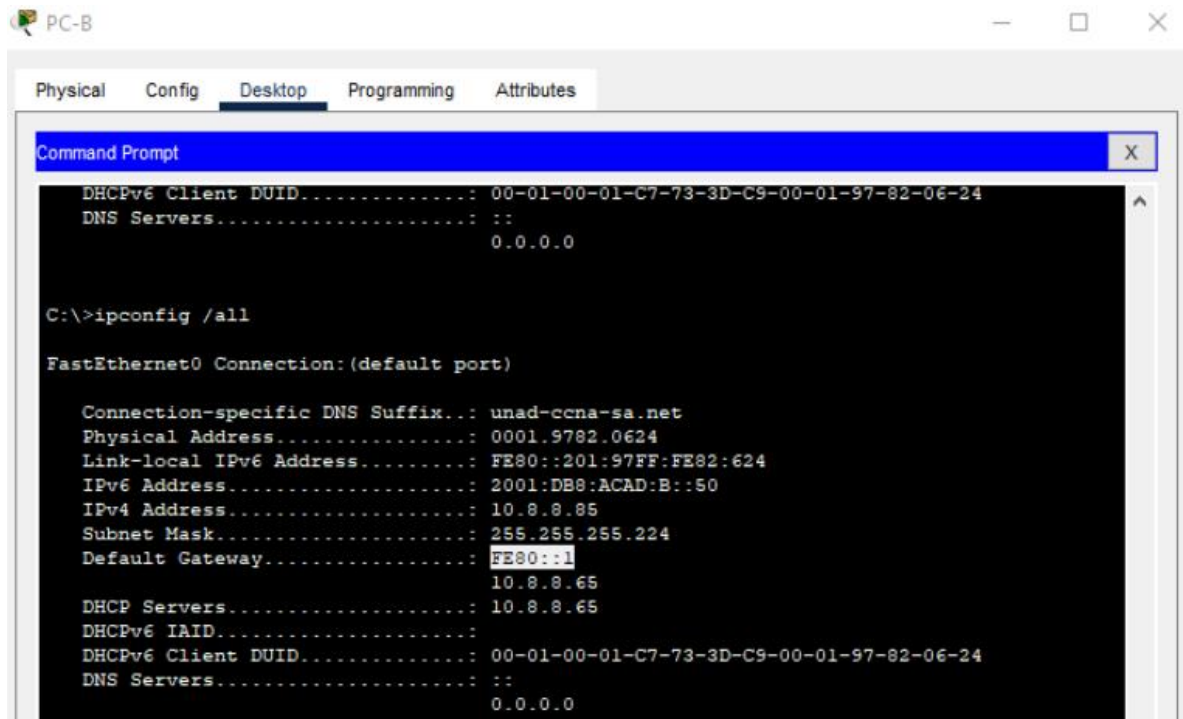
Fuente Autoría propia

Tabla 25. Configuración red de PC-B

| Configuración de red de PC-B | |
|------------------------------|-----------------|
| Descripción | |
| Dirección física | 0001.9782.0624 |
| Dirección ip | 10.8.8.85 |
| Mascara de subred | 255.255.255.224 |
| Gateway predeterminado | 10.8.8.65 |
| Gateway predeterminado IPV6 | FE80::1 |

Fuente Autoría propia

Figura 28 ipconfig PC-B Escenario 2

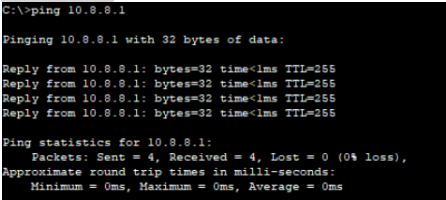
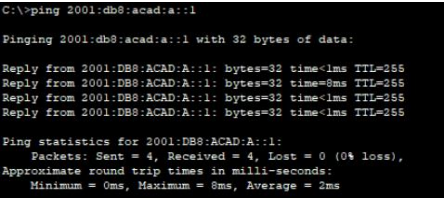
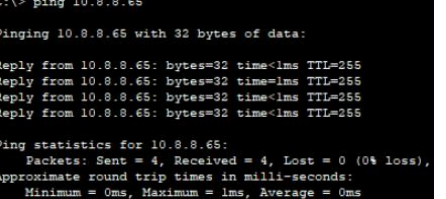
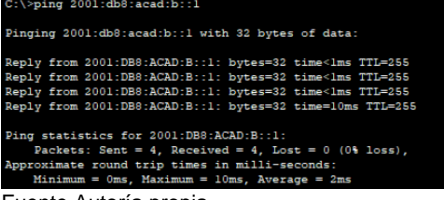


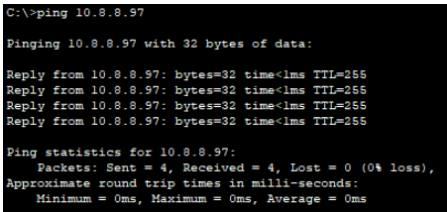
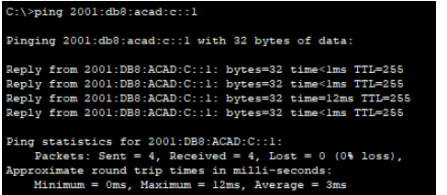
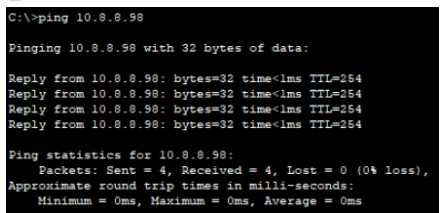
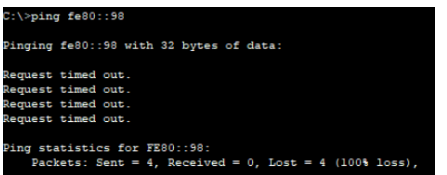
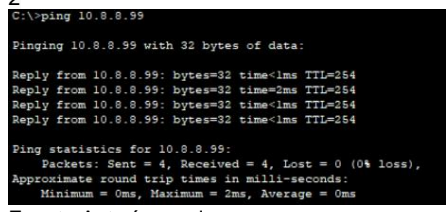
Fuente Autoría propia

2.9 Probar y verificar la conectividad de extremo a extremo

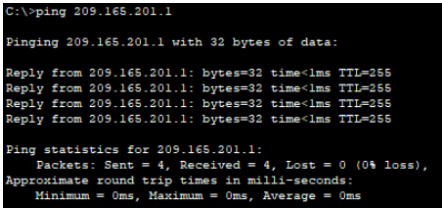
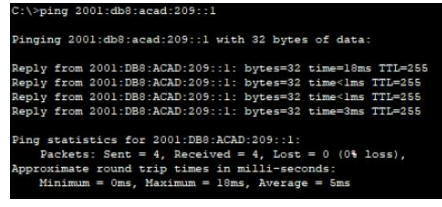
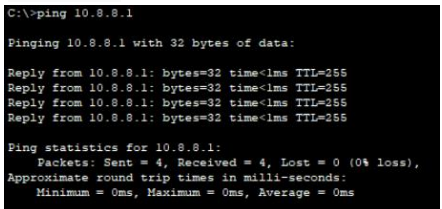
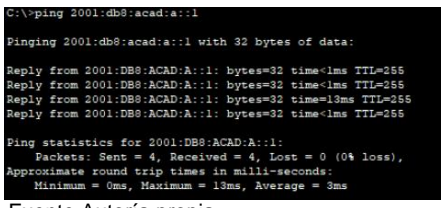
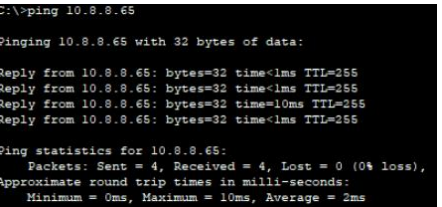
Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 26. Verificación de conectividad

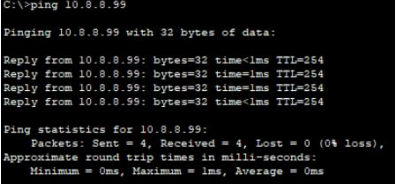
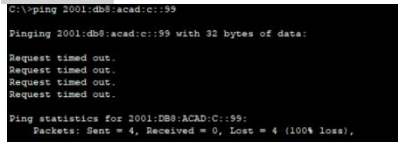
| Desde | A | | Dirección IP | Resultados de ping |
|-------|------------------------------------|------|--------------------|--|
| PC-A | R1, G0/0/1.2 R1, G0/0/1.2 | IPv4 | 10.8.8.1 | <p>Figura 29 ping IPV4 PC-A R1 G0/0/1.2 Escenario 2</p>  <p>Fuente Autoría propia</p> |
| | | IPv6 | 2001:db8:acad:a::1 | <p>Figura 30 ping IPV6 PC-A R1 G0/0/1.2 Escenario 2</p>  <p>Fuente Autoría propia</p> |
| | R1, G0/0/1.3 R1, G0/0/1.3 | IPv4 | 10.8.8.65 | <p>Figura 31 ping IPV4 PC-A R1 G0/0/1.3 Escenario 2</p>  <p>Fuente Autoría propia</p> |
| | | IPv6 | 2001:db8:acad:b::1 | <p>Figura 32 ping IPV6 PC-A R1 G0/0/1.3 Escenario 2</p>  <p>Fuente Autoría propia</p> |
| | | IPv4 | 10.8.8.97 | |

| | | | | |
|-------|------------------------------------|------|---------------------|--|
| | R1, G0/0/1.4 R1, G0/0/1.4 | | | <p>Figura 33 ping IPV4 PC-A R1 G0/0/1.4 Escenario 2</p>  <p>Fuente Autoría propia</p> |
| | | IPv6 | 2001:db8:acad:c::1 | <p>Figura 34 ping IPV6 PC-A R1 G0/0/1.4 Escenario 2</p>  <p>Fuente Autoría propia</p> |
| | S1, VLAN 4 S1, VLAN 4 | IPv4 | 10.8.8.98 | <p>Figura 35 ping IPV4 PC-A S1 VLAN4 Escenario 2</p>  <p>Fuente Autoría propia</p> |
| | | IPv6 | 2001:db8:acad:c::98 | <p>Figura 36 ping IPV6 PC-A S1 VLAN4 Escenario 2</p>  <p>Fuente Autoría propia</p> |
| Desde | A | | Dirección IP | Resultados de ping |
| PC-A | S2, VLAN 4 S2, VLAN 4 | IPv4 | 10.8.8.99 | <p>Figura 37 ping IPV4 PC-A S2 VLAN4 Escenario 2</p>  <p>Fuente Autoría propia</p> |

| | | | | |
|--|--------------------------------|------|----------------------|--|
| | | IPv6 | 2001:db8:acad:c::99 | <p>Figura 38 ping IPV6 PC-A S2 VLAN4 Escenario 2</p> <pre>C:\>ping 2001:db8:acad:c::99 Pinging 2001:db8:acad:c::99 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 2001:DB8:ACAD:C::99: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),</pre> <p>Fuente Autoría propia</p> |
| | PC-B PC-B | IPv4 | 10.8.8.85 | <p>Figura 39 ping IPV4 PC-A PC-B Escenario 2</p> <pre>C:\> ping 10.8.8.85 Pinging 10.8.8.85 with 32 bytes of data: Reply from 10.8.8.85: bytes=32 time<1ms TTL=127 Reply from 10.8.8.85: bytes=32 time<1ms TTL=127 Reply from 10.8.8.85: bytes=32 time<1ms TTL=127 Reply from 10.8.8.85: bytes=32 time<1ms TTL=127 Ping statistics for 10.8.8.85: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> <p>Fuente Autoría propia</p> |
| | | IPv6 | 2001:db8:acad:b::50 | <p>Figura 40 ping IPV6 PC-A PC-B Escenario 2</p> <pre>C:\>ping 2001:db8:acad:b::50 Pinging 2001:db8:acad:b::50 with 32 bytes of data: Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127 Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127 Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127 Reply from 2001:DB8:ACAD:B::50: bytes=32 time<1ms TTL=127 Ping statistics for 2001:DB8:ACAD:B::50: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 10ms, Average = 2ms</pre> <p>Fuente Autoría propia</p> |
| | R1 Bucle 0 R1 Bucle 0 | IPv4 | 209.165.201.1 | <p>Figura 41 ping IPV4 PC-A R1 BUCLE Escenario 2</p> <pre>C:\>ping 209.165.201.1 Pinging 209.165.201.1 with 32 bytes of data: Reply from 209.165.201.1: bytes=32 time<1ms TTL=255 Reply from 209.165.201.1: bytes=32 time<1ms TTL=255 Reply from 209.165.201.1: bytes=32 time<1ms TTL=255 Reply from 209.165.201.1: bytes=32 time<1ms TTL=255 Ping statistics for 209.165.201.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> <p>Fuente Autoría propia</p> |
| | | IPv6 | 2001:db8:acad:209::1 | <p>Figura 42 ping IPV6 PC-A R1 BUCLE Escenario 2</p> <pre>C:\>ping 2001:db8:acad:209::1 Pinging 2001:db8:acad:209::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms TTL=255 Ping statistics for 2001:DB8:ACAD:209::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> <p>Fuente Autoría propia</p> |

| | | | | |
|------------------------------------|--------------------------|------|----------------------|--|
| PC-B | R1 Bucle 0 R1 Bucle 0 | IPv4 | 209.165.201.1 | <p>Figura 43 ping IPV4 PC-B R1BUCLE Escenario 2</p>  <p>Fuente Autoría propia</p> |
| | | IPv6 | 2001:db8:acad:209::1 | <p>Figura 44 ping IPV6 PC-B R1 BUCLE Escenario 2</p>  <p>Fuente Autoría propia</p> |
| R1, G0/0/1.2 R1, G0/0/1.2 | | IPv4 | 10.8.8.1 | <p>Figura 45 ping IPV4 PC-B R1 G0/0/1.2 Escenario 2</p>  <p>Fuente Autoría propia</p> |
| | | IPv6 | 2001:db8:acad:a::1 | <p>Figura 46 ping IPV6 PC-B R1 G0/0/1.2 Escenario 2</p>  <p>Fuente Autoría propia</p> |
| R1, G0/0/1.3 R1, G0/0/1.3 | | IPv4 | 10.8.8.65 | <p>Figura 47 ping IPV4 PC-B R1 G0/0/1.3 Escenario 2</p>  <p>Fuente Autoría propia</p> |

| | | | | |
|------------------------------------|--|------|---------------------|---|
| | | IPv6 | 2001:db8:acad:b::1 | <p>Figura 48 ping IPV6 PC-B R1 G0/0/1.3</p> <pre>C:\>ping 2001:db8:acad:b::1 Pinging 2001:db8:acad:b::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255 Ping statistics for 2001:DB8:ACAD:B::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> <p>Escenario 2 Fuente Autoría propia</p> |
| R1, G0/0/1.4 R1, G0/0/1.4 | | IPv4 | 10.8.8.97 | <p>Figura 49 ping IPV4 PC-B R1 G0/0/1.4 Escenario 2</p> <pre>C:\>ping 10.8.8.97 Pinging 10.8.8.97 with 32 bytes of data: Reply from 10.8.8.97: bytes=32 time<1ms TTL=255 Reply from 10.8.8.97: bytes=32 time<1ms TTL=255 Reply from 10.8.8.97: bytes=32 time<1ms TTL=255 Reply from 10.8.8.97: bytes=32 time<1ms TTL=255 Ping statistics for 10.8.8.97: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> <p>Fuente Autoría propia</p> |
| | | IPv6 | 2001:db8:acad:c::1 | <p>Figura 50 ping IPV6 PC-B R1 G0/0/1.4 Escenario 2</p> <pre>C:\>ping 2001:db8:acad:c::1 Pinging 2001:db8:acad:c::1 with 32 bytes of data: Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255 Reply from 2001:DB8:ACAD:C::1: bytes=32 time<1ms TTL=255 Ping statistics for 2001:DB8:ACAD:C::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre> |
| S1, VLAN 4 S1, VLAN 4 | | IPv4 | 10.8.8.98 | <p>Figura 51 ping IPV4 PC-B S1 VLAN4</p> <pre>C:\>ping 10.8.8.98 Pinging 10.8.8.98 with 32 bytes of data: Reply from 10.8.8.98: bytes=32 time<1ms TTL=254 Reply from 10.8.8.98: bytes=32 time<1ms TTL=254 Reply from 10.8.8.98: bytes=32 time<1ms TTL=254 Reply from 10.8.8.98: bytes=32 time=5ms TTL=254 Ping statistics for 10.8.8.98: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 5ms, Average = 2ms</pre> <p>Escenario 2 Fuente Autoría propia</p> |
| | | IPv6 | 2001:db8:acad:c::98 | <p>Figura 52 ping IPV6 PC-B S1 VLAN4 Escenario 2</p> <pre>C:\>ping 2001:db8:acad:c::98 Pinging 2001:db8:acad:c::98 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 2001:DB8:ACAD:C::98: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),</pre> <p>Fuente Autoría propia</p> |

| | | | | |
|--|--------------------------------|------|---------------------|---|
| | S2, VLAN 4 S2, VLAN 4 | IPv4 | 10.8.8.99 | <p>Figura 53 ping IPV4 PC-B S2 VLAN4 Escenario 2</p>  <p>Fuente Autoría propia</p> |
| | | IPv6 | 2001:db8:acad:c::99 | <p>Figura 54 ping IPV6 PC-B S2 VLAN4 Escenario 2</p>  <p>Fuente Autoría propia</p> |

Fuente Autoría propia

Se realizaron pruebas de conexión mediante el comando ping entre el PC-A y interfaces de conexión del R1, S1, S2 y PC-B permitiendo verificar la correcta conectividad entre los mismo.

De igual manera se realizaron pruebas para verificar conexión entre PC-B e interfaces de R1, S1, S2 permitiendo verificar la correcta conectividad entre los mismo.

CONCLUSIONES

El objetivo guía del presente trabajo era crear, simular y configurar cada uno de los escenarios propuestos, el cual se cumplió con la implementación de los mismo y su respectiva explicación a través de este documento.

Se logro la implementación de los escenarios por medio de la utilización del software de simulación Packet Tracer permitiendo emular las redes propuestas de acuerdo a los dispositivos que la componían y el tipo de conexión que necesitaban.

La implementación del escenario 1 permitió simular una red básica compuesta por un Router, switch y equipos de cómputo y creaciones de VLANs los cuales se realizó la configuración para permitir la comunicación de los mismos a través del protocolo IPV4

La implementación del escenario 2 permitió simular una red compuesta por un Router, 2 switches, equipos de cómputo, creación de VLANs, configuración de DHCP, Etherchannel y portsecurity permitiendo la comunicación de los mismos a través del protocolo IPV4, IPV6 y su respectiva verificación de comunicación

Se comprendió los conceptos de direccionamiento ipv6 y ipv4, el proceso de subnetting y su implementación.

BIBLIOGRAFÍA

Abad, D. A. "Redes locales". {En línea}. (2010). {10, diciembre de 2022}. Disponible en: <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/50228?page=81>

Castaño, R. R. J., y López, F. J. "Redes locales". {En línea}. (2013). {10, diciembre de 2022}. Disponible en: <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=159>

CISCO. "Asignación de direcciones IPv4. Introducción a las redes". {En línea}. (2020). {10, diciembre de 2022}. Disponible en: <https://contenthub.netacad.com/itn/11.0.1>

CISCO. "Asignación de direcciones IPv6. Introducción a las redes". {En línea}. (2020). {10, diciembre de 2022}. Disponible en: <https://contenthub.netacad.com/itn/12.0.1>

CISCO. "Capa de red. Introducción a las redes". {En línea}. (2020). {10, diciembre de 2022}. Disponible en: <https://contenthub.netacad.com/itn/8.0.1>

CISCO. "Configuración básica de un Router. Introducción a las redes". {En línea}. (2020). {10, diciembre de 2022}. Disponible en: <https://contenthub.netacad.com/itn/10.0.1>

CISCO. "ICMP. Introducción a las redes". {En línea}. (2020). {10, diciembre de 2022}. Disponible en: <https://contenthub.netacad.com/itn/13.0.1>

CISCO. "Resolución de dirección. Introducción a las redes". {En línea}. (2020). {10, diciembre de 2022}. Disponible en: <https://contenthub.netacad.com/itn/9.0.1>

ANEXOS

ANEXO A – Enlace de descarga de las simulaciones de los escenarios.

[habilidadesf.zip](#)